REMARKS

The following remarks are prepared in response to the final Office Action of October 17, 2005. Claims 1-10 remain pending in this application, after entry of this amendment. Reconsideration in light of the remarks made herein is respectfully requested.

Rejection of Claims 1-6 and 9-10 Under 35 U.S.C. § 102(b)

Claims 1-6 and 9-10 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Wasilewski et al.* (U.S. Patent No. 5,870,474, hereinafter *Wasilewski*). Applicant respectfully traverses.

Combination of Elements Are Patentable Over Wasilewski

The Examiner should consider the combination of the updating, generating and encrypting means to be patentable. The Examiner is making an incorrect analogy between terms recited in the claims and terms disclosed in *Wasilewski*. The following chart points out the differences between the terms.

Term in Claim	**Term in Wasilewski**	**Difference**
Type 1 Key	Multi-Session Key (MSK)	Type 1 Key is updated in response to usage of the main data read from the recording medium. MSK is updated in the order of once a day or once a month.
Type 2 Key	Control Word	Type 2 Key is updated in response to usage of the main data read from the recording medium. Control Word is a random number updated every few seconds.
Main Data	Payload	Main Data is unchanged in the recording medium. Payload is the contents of the TS packets and differs from time to

		time.
Condition Information	Control Word	Condition Information is updated in response to usage of the main data. Control Word is a random number updated every few seconds.

These terms recited in the claims are closely related to one another and simple picking and choosing terms from *Wasilewski* does not teach or suggest the features recited in the claims.

Independent Claim 1

Independent claim 1 recites "first updating means for updating the condition information in accordance with usage of the read main data." The condition information is updated in accordance with usage of the "main data" read from the recording medium. The condition information, as well as other claimed elements, aims to prevent the backup and restore attack even by an initially authorized user. For example, a user may use the main data in excess of its initially set condition by backing up (i.e., copying) and later restoring the condition information. The backup and restore attack is illegal in that although the main data has been actually used, the restored condition information reflects the state before such usage. However, by updating the condition information in accordance with usage of the main data (and updating the type 1 key and encrypting the type 2 key — discussed below), the user is unable to excessively use the main data. Hence, the condition information is used to restrict the number of executions permitted for the "main data" read from the recording medium.

Wasilewski does not update its control words in accordance with usage of the main data. On page 3 of the final Office Action, the Examiner directs Applicant to col. 8, lns. 48-60 for this feature; however, this paragraph states that the control words change most often (e.g., every few seconds) because if an unauthorized user came into possession of a control word, that control word would expire before any advantage could be gained. Furthermore, this paragraph states that the control word changes often and the encryption must be performed quickly to keep up with the high program data rates. Nothing is disclosed in *Wasilewski* about updating the control words based on usage of the main data. Thus, the condition information recited in independent claim 1 and the control words disclosed in *Wasilewski* are not the same and cannot be referred to as being the same. Furthermore, the condition information recited in independent claim 1 and the MSK or the payload disclosed in *Wasilewski* are not the same and cannot be referred to as being the same.

Independent claim 1 also recites "second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key." The type 1 key is updated in the storage unit (not in the recording medium) in accordance with the usage of the read main data. The type 1 key is updated by the second updating means, and the type 2 key, which is used for encrypting the condition information in the recording medium, is encrypted using the updated type 1 key. Then, the type 2 key in the recording medium is replaced with the newly encrypted type 2 key by the second encrypting means. Specifically, the type 1 key in a predetermined storage unit is updated according to the usage of the main data in a system in which (i) the encrypted type 2 key in the recording medium is decoded based on the type 1 key in a predetermined storage unit, (ii) the encrypted condition information is decoded using the decoded type 2 key, and (iii) thereby controlling the usage of the main data based on the obtained condition information. Consequently, the backed-up condition information and the type 2 key are no longer valid, and thus unauthorized use by the backup and restore attack is prevented.

Moreover, the type 1 key is used by the second encrypting means to encrypt the type 2 key. Therefore, even if assuming the type 1 key is equivalent to the public key or private key used in the public-key encryption algorithm that is used to encrypt the MSK of *Wasilewski*, this assumption turns out to be incorrect because the type 1 key is updated by the second updating means in accordance with the usage of the main data, while the public key or private key in the set top unit (STU) is not updated in accordance with the usage of the main data in *Wasilewski*.

Accordingly, *Wasilewski* does not disclose a data usage controlling apparatus that decrypts the encrypted condition information using the type 2 key and includes second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key. For at least the reasons discussed above, Applicant submits that independent claim 1 is patentably distinct over *Wasilewski* and the rejection under 35 U.S.C. § 102(b) should be withdrawn.

Independent Claims 2, 9 and 10

Independent claims 2, 9 and 10 include similar features as recited in independent claim 1. For example, claim 2 is similar to claim 1, claim 9 is a data usage controlling method that corresponds to claim 1, and claim 10 is a computer-readable recording medium storing a program that corresponds to claim 1. Therefore, for at least this reason and the reasons discussed above for independent claim 1, Applicant submits that claims 2, 9 and 10 are patentably distinct over *Wasilewski* and the rejection under 35 U.S.C. § 102(b) should be withdrawn.

Dependent Claims 3-8

Claims 3-8 depend from independent claim 2, adding structural features that more particularly define the invention and further distinguish over the cited references and the prior art of record. For these reasons, and for the reasons set forth above for independent claim 2, the rejection of these dependent claims under 35 U.S.C. §§ 102(b) and 103(a) are improper and should be withdrawn.

Conclusion

If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 17, 2006.

By: Tanya Kiatkulpiboone

Signature

Dated: January 17, 2006

Very truly yours,

SNELL & WILMER L.L.P.

Ketan S Vakil

Ketan S. Vakil
Registration No. 43,215
600 Anton Boulevard, Suite 1400
Costa Mesa, CA 92626-7689
Telephone: (714) 427-7405